**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

CASSIOPEIA IP LLC,

        Plaintiff,

        v.

SEAGATE TECHNOLOGY LLC,

        Defendant.

Civil Action No.:

TRIAL BY JURY DEMANDED

COMPLAINT FOR INFRINGEMENT OF PATENT

Now comes, Plaintiff Cassiopeia IP LLC ("Plaintiff" or "Cassiopeia"), by and through undersigned counsel, and respectfully alleges, states, and prays as follows:

NATURE OF THE ACTION

1.   This is an action for patent infringement under the Patent Laws of the United States, Title 35 United States Code ("U.S.C.") to prevent and enjoin Defendant Seagate Technology LLC (hereinafter "Defendant"), from infringing and profiting, in an illegal and unauthorized manner, and without authorization and/or consent from Plaintiff from U.S. Patent No. 7,322,046 ("the '046 Patent" or the "Patent-in-Suit"), which is attached hereto as Exhibit A and incorporated herein by reference, and pursuant to 35 U.S.C. §271, and to recover damages, attorney's fees, and costs.

THE PARTIES

2.   Plaintiff is a Texas limited liability company with its principal place of business at 6009 West Parker Road – Suite 149-1038, Plano, Texas 75093-8121.

3.   Upon information and belief, Defendant is a corporation organized under the laws of Delaware, having a principal place of business at 47488 Kato Road, Fremont, California 94538. Upon information and belief, Defendant may be served with process c/o The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801.

4.   Plaintiff is further informed and believes, and on that basis alleges, that Defendant operates the website www.seagate.com, which is in the business of providing consumer electronics using secure network services. Defendant derives a portion of its revenue from sales and distribution via electronic transactions conducted on and using at least, but not limited to, its Internet website located at www.seagate.com, and its incorporated and/or related systems or products (collectively the "Seagate Website"). Plaintiff is informed and believes, and on that basis alleges, that, at all times relevant hereto, Defendant has done and continues to do business in this judicial district, including, but not limited to, providing products/services to customers located in this judicial district by way of the Seagate Website.

JURISDICTION AND VENUE

5.   This is an action for patent infringement in violation of the Patent Act of the United States, 35 U.S.C. §§1 *et seq*.

6.   The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§1331 and 1338(a).

7.   This Court has personal jurisdiction over Defendant by virtue of its systematic and continuous contacts with this jurisdiction and its residence in this District, as well as because of the injury to Plaintiff, and the cause of action Plaintiff has risen in this District, as alleged herein.

8.   Defendant is subject to this Court's specific and general personal jurisdiction pursuant to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Delaware and in this judicial District; and (iii) being incorporated in this District.

9.   Venue is proper in this judicial district pursuant to 28 U.S.C. §1400(b) because Defendant resides in this District under the Supreme Court's opinion in *TC Heartland v. Kraft Foods Group Brands LLC,* 137 S. Ct. 1514 (2017) through its incorporation, and regular and established place of business in this District.

FACTUAL ALLEGATIONS

10.   On January 22, 2008, the United States Patent and Trademark Office ("USPTO") duly and legally issued the '046 Patent, entitled "METHOD AND SYSTEM FOR THE SECURE USE OF A NETWORK SERVICE" after a full and fair examination. The '046 Patent is attached hereto as Exhibit A and incorporated herein as if fully rewritten.

11.   Plaintiff is presently the owner of the '046 Patent, having received all right, title and interest in and to the '046 Patent from the previous assignee of record. Plaintiff possesses all rights of recovery under the '046 Patent, including the exclusive right to recover for past infringement.

12.   To the extent required, Plaintiff has complied with all marking requirements under 35 U.S.C. § 287.

13.   The invention claimed in the '046 Patent comprises a method for the secure use of a network service using a blackboard on which all usable services are entered.

14.   Claim 1 of the '046 Patent states:

"1. A method for the secure use of a network service using a blackboard on which all usable services are entered, the method comprising the steps of: detecting a service which has not yet been entered on the blackboard; executing a first check to determine whether use of the service is allowed; entering the service in the blackboard only if it is determined that use of the service is allowed; loading an interface driver related to the service on the blackboard; extending the loaded interface driver on the blackboard with at least one security function to form a secured interface driver; loading the secured interface driver related to the service prior to the first use of the service; and executing a second check by a second security function prior to the use of the service to determine if use of the service is allowed by a user." *See* Exhibit A.

15.   Defendant commercializes, inter alia, methods that perform all the steps recited in at least one claim of the '046 Patent. More particularly, Defendant commercializes, inter alia, methods that perform all the steps recited in Claim 1 of the '046 Patent. Specifically, Defendant makes, uses, sells, offers for sale, or imports a method that encompasses that which is covered by Claim 1 of the '046 Patent.

DEFENDANT'S PRODUCTS

16.   Defendant offers solutions, such as "Seagate Central" (the "Accused Product"), that enables a method for the secure use of a network service using a blackboard on which all usable services are entered. For example, the Accused Product performs the method for the secure use of a network service using a blackboard on which all usable services are entered. A non-limiting and exemplary claim chart comparing the Accused Product to Claim 1 of the '046 Patent is attached hereto as Exhibit B and is incorporated herein as if fully rewritten.

4

17.   As recited in Claim 1, upon information and belief, and in at least testing and usage, the Accused Product serves as a DLNA client (e.g., projects media transmitted from other DLNA devices) which practices a method for secure use of a network service (e.g., various services provided by DLNA enabled servers) using a blackboard (e.g., a software/hardware component that stores all available DLNA services and corresponding servers/devices, among others) on which all usable services (e.g., services provided by DLNA servers) are entered. The Accused Product supports DLNA and can project media from mobile devices, cameras, and other devices which are DLNA compatible. DLNA utilizes UPnP device architecture and UPnP's service and device discovery mechanism to discover various devices and corresponding services available on a network. SSDP protocol (Simple Service Discovery Protocol) is used by UPnP devices to discover services available from UPnP servers (e.g., DLNA servers in DLNA networks). The DLNA protocol allows a DLNA client (e.g., an UPnP control point) to discover DLNA services provided by DLNA servers (e.g., UPnP servers/devices). On information and belief, the accused product, in its internal testing and usage, utilizes a DLNA client which must utilize a blackboard (e.g. database or lookup table) that stores services provided by discovered DLNA servers. *See* Exhibit B.

18.   As recited in one step of Claim 1, upon information and belief, the Accused Product utilizes a DLNA client (e.g., an UPnP control point) which will send out an M-SEARCH to discover DLNA servers (e.g., UPnP servers/devices). In response, a DLNA server (e.g., an UPnP server/device) will send a response with a location header that includes an HTTP URL that holds an UPnP description of the DLNA server (e.g., an UPnP servers/device). The DLNA client (e.g., an UPnP control point) will then send a HTTP GET message to the HTTP URL in the

location header. If the HTTP GET is sent to the correct HTTP URL originally provided by the DLNA server (e.g., an UPnP server/device), the DLNA server (e.g., an UPnP servers/device) will send the DLNA client (e.g., an UPnP control point) that identifies the services a client can utilize. The response of the DLNA server (e.g., an UPnP server/device) includes a list of the commands, or actions, the service responds to, and parameters, or arguments, for each action; the description for a service also includes a list of variables; these variables model the state of the service at run time, and are described in terms of their data type, range, and event characteristics. As such the service, offered by the DLNA server (e.g., an UPnP server) identified by the DLNA client (e.g., an UPnP control point) is added to the blackboard. Further, the DLNA client can invoke actions through HTTP methods using the controlURL sub element of service element of device description provided by the DLNA server (e.g., an UPnP server/device). The DLNA client further is also configured to load a presentation page to its browser to invoke actions from DLNA server (e.g., UPnP server). *See* Exhibit B.

19.   As recited in another step of Claim 1, upon information and belief, the Accused Product utilizes a system in which a first check is executed to determine whether a use of the service is allowed. A DLNA client (e.g., an UPnP control point) sends out an M-SEARCH that defines particular services that the client is looking for. A DLNA server (e.g., an UPnP server/device) will only respond to this request if they provide services that the client is searching for. This serves as a first check that ensures that the services provided by a DLNA server (e.g., UPnP server/device) responding to the client can in fact be used by the client. *See* Exhibit B.

20.   As recited in another step of Claim 1, upon information and belief, the Accused Product will only enter the service (e.g., access to DLNA server and its services) in the blackboard (e.g. a database or list of available servers/services) only if it is determined that the use of the service is allowed (e.g. the server/service responding to a client request matches the service defined in the request). *See* Exhibit B.

21.   As recited in another step of Claim 1, upon information and belief, the Accused Product utilizes a system that loads an interface driver related to the service on the blackboard (e.g. the client's receipt of a control and presentation URLs of the service offered by the DLNA server identifies the services that can be provided by the DLNA server). The client's receipt of the controlURL allows the client to interface with the DLNA server in order to invoke a service related action on the said DLNA server. The DLNA client further is also configured to load a presentation page to its browser to invoke actions from the DLNA server (e.g., UPnP server). A DLNA client (e.g., an UPnP control point) will send out an M-SEARCH to discover DLNA servers (e.g., UPnP servers/devices). In response, a DLNA server (e.g., an UPnP servers/device) will send a response with a location header that includes an HTTP URL that holds an UPnP description of the DLNA server (e.g., an UPnP server/device). The DLNA client (e.g., an UPnP control point) will then send a HTTP GET message to the HTTP URL in the location header. If the HTTP GET is sent to the correct HTTP URL originally provided by the DLNA server (e.g., an UPnP servers/device), the DLNA server (e.g., an UPnP servers/device) will send the DLNA client (e.g., an UPnP control point) that identifies the services a client can utilize. The response of the DLNA server (e.g., an UPnP server/device) includes a list of the commands, or actions, the service responds to, and parameters, or arguments, for each action; the description for a

service also includes a list of variables; these variables model the state of the service at run time, and are described in terms of their data type, range, and event characteristics. As such the service, offered by the DLNA server (e.g., an UPnP server) identified by the DLNA client (e.g., an UPnP control point) is added to the blackboard. Further, the DLNA client can invoke actions through HTTP methods using the controlURL sub element of service element of device description provided by the DLNA server (e.g., an UPnP server/device). *See* Exhibit B.

22.   As recited in another step of Claim 1, upon information and belief, the Accused Product practices extending the loaded interface driver (e.g., ControlURL which can invoke actions related to a service from the DLNA server and   the presentationURL which loads a presentation page to invoke actions related to a service from the DLNA server) on the blackboard (e.g., a software/hardware component which logs services and service software) with at least one security function (e.g., the verification of the signature of the DLNA client (e.g., UPnP control point/sender) to form a secured interface driver (e.g., upon signature verification, DLNA server will allow the DLNA client to invoke actions and also subsequently load presentation page to control/invoke an action from DLNA server). *See* Exhibit B.

23.   As recited in another step of Claim 1, upon information and belief, the Accused Product loads to the DLNA client the secured interface driver related to the service prior to the first use of the service (e.g., upon signature verification, the DLNA client (e.g., UPnP control point) loads presentation page to control/invoke an action related to a service from DLNA server) and executing a second check (e.g., a check to determine if the action related to the service requires authorization and the DLNA client is not authorized) by a second security

function (e.g., action specific authorization) prior to the use of the service to determine if use of the service is allowed by a user. *See* Exhibit B.

24.   The elements described in the preceding paragraphs are covered by at least Claim 1 of the '046 Patent. Thus, Defendant's use of the Accused Product is enabled by the method described in the '046 Patent.

INFRINGEMENT OF THE '046 PATENT

25.   Plaintiff realleges and incorporates by reference all of the allegations set forth in the preceding Paragraphs.

26.   In violation of 35 U.S.C. § 271, Defendant is now, and has been directly infringing the '046 Patent.

27.   Defendant has had knowledge of infringement of the '046 Patent at least as of the service of the present Complaint.

28.   Defendant has directly infringed and continues to directly infringe at least one claim of the '046 Patent by using, at least through internal testing or otherwise, the Accused Product without authority in the United States, and will continue to do so unless enjoined by this Court. As a direct and proximate result of Defendant's direct infringement of the '046 Patent, Plaintiff has been and continues to be damaged.

29.   By engaging in the conduct described herein, Defendant has injured Plaintiff and is thus liable for infringement of the '046 Patent, pursuant to 35 U.S.C. § 271.

30.   Defendant has committed these acts of infringement without license or authorization.

31.   As a result of Defendant's infringement of the '046 Patent, Plaintiff has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate for Defendant's past infringement, together with interests and costs.

32.   Plaintiff will continue to suffer damages in the future unless Defendant's infringing activities are enjoined by this Court. As such, Plaintiff is entitled to compensation for any continuing and/or future infringement up until the date that Defendant is finally and permanently enjoined from further infringement.

33.   Plaintiff reserves the right to modify its infringement theories as discovery progresses in this case; it shall not be estopped for infringement contention or claim construction purposes by the claim charts that it provides with this Complaint. The claim chart depicted in Exhibit B is intended to satisfy the notice requirements of Rule 8(a)(2) of the Federal Rule of Civil Procedure and does not represent Plaintiff's preliminary or final infringement contentions or preliminary or final claim construction positions.

DEMAND FOR JURY TRIAL

34.   Plaintiff demands a trial by jury of any and all causes of action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

a.   That Defendant be adjudged to have directly infringed the '046 Patent either literally or under the doctrine of equivalents;

b.   An accounting of all infringing sales and damages including, but not limited to, those sales and damages not presented at trial;

c. That Defendant, its officers, directors, agents, servants, employees, attorneys, affiliates, divisions, branches, parents, and those persons in active concert or participation with any of them, be permanently restrained and enjoined from directly infringing the '046 Patent;

d. An award of damages pursuant to 35 U.S.C. §284 sufficient to compensate Plaintiff for the Defendant's past infringement and any continuing or future infringement up until the date that Defendant is finally and permanently enjoined from further infringement, including compensatory damages;

e. An assessment of pre-judgment and post-judgment interest and costs against Defendant, together with an award of such interest and costs, in accordance with 35 U.S.C. §284;

f. That Defendant be directed to pay enhanced damages, including Plaintiff's attorneys' fees incurred in connection with this lawsuit pursuant to 35 U.S.C. §285; and

g. That Plaintiff be granted such other and further relief as this Court may deem just and proper.

Dated: October 26, 2020

Together with:

SAND, SEBOLT & WERNOW CO., LPA

Andrew S. Curfman
(*pro hac vice forthcoming*)

Aegis Tower – Suite 1100
4940 Munson Street NW
Canton, Ohio 44718
Telephone: (330) 244-1174
Facsimile: (330) 244-1173
andrew.curfman@sswip.com

Respectfully submitted,

CHONG LAW FIRM PA

/s/ Jimmy Chong
Jimmy Chong (#4839)
2961 Centerville Road, Suite 350
Wilmington, Delaware 19808
Telephone: (302) 999-9480
Facsimile: (877) 796-4627
Email:chong@chonglawfirm.com

ATTORNEYS FOR PLAINTIFF